Towards the Integration of Safety Analysis in a Model-Based System Engineering Approach with SysML

Faida Mhenni, Nga Nguyen, Jean-Yves Choley

Towards the Integration of Safety Analysis in a Model-Based System Engineering Approach with SysML

Faïda Mhenni[1], Nga Nguyen[2], Jean-Yves Choley[1]

[1] LISMMA – SUPMECA, 3 rue Fernand Hainaut, 93400 Saint-Ouen, France

{faida.mhenni, jean-yves.choley}@supmeca.fr

[2] Laris – Eisti, Avenue du Parc, 95000 Cergy Pontoise, France

nn@eisti.eu

Abstract. Mechatronic systems are complex systems involving knowledge from various disciplines such as computer science, mechanics, electronics and control. Model-based system engineering is an efficient approach to cope with the increasing system complexity. It covers specifying, designing, simulating and validating systems and is very useful for the design of complex systems since it helps better manage the complexity while enhancing consistency and coherence. This approach allows errors to be detected as soon as possible in the design process, and thus reduces the overall cost of the product. Integrating safety concerns from early design stages, within the MBSE approach helps the designer to consider safety aspect during system architecture synthesis and reduce the number of iterations and design changes. This paper presents a step towards the integration of safety within the MBSE approach. SysML is chosen as a modeling language because it offers unified communication semantics to the multidisciplinary collaborating team involved in the design of complex systems. A case study illustrates the proposed approach.

Keywords: safety analysis, SysML, MBSE.

1 Introduction

Nowadays manmade systems are getting more complex, achieving more functions and thus involving an increasing number of components and new technologies. Components of different disciplines such as actuators, sensors, software are interacting together in a synergic way. In such interactively complex systems,

there are many branching paths among components making the interactions unpredictable to system designers and users. Therefore, complex systems are error prone and safety critical since errors could lead to accidents with potentially catastrophic effects. Normal Accident Theory (NAT) explains that, when a technology becomes sufficiently complex and tightly coupled, accidents become inevitable and therefore in a sense they become 'normal' (Perrow1981).

Consequently, the design of such systems is challenging. Firstly, the increasing complexity of manufactured systems makes their development and safety analysis more difficult and big efforts are required to manage the complexity, maintaining coherence and consistency through the development, and deal with numerous requirements relevant to multiple domains. Moreover, safety critical systems must be certified according to continuously more rigorous safety regulations before commercialization. In addition, sharp industrial competitiveness obliges industrials to shorten time to market and reduce development costs. Communication among the engineering team working together is also challenging. In fact, engineers from different fields and with different technological backgrounds cooperate together during the design process. This usually leads to misunderstanding and confusion.

Model-Based System Engineering (MBSE) approach is required to manage the complexity, enhance consistency and allow modeling and simulation of the whole system. A unified language to model and specify the system will remedy to the communication problem; SysML, the semi-formal systems modeling language seems very appropriate for us and is adapted in our work.

2 Related work

As manufactured systems began to be more widely used, an as manmade system cannot be perfect and are subject to different kind of malfunction, – caused either by design errors, human errors, component failure or any other direct cause or combination of contributing events – many research works focused on system safety. The first efforts were noted in the military domain leading for instance to the military standards (MIL-STD-1629A , MIL-STD-882D). The aim of such standards is to help designers in identifying potential hazards and the appropriate corrective actions. Safety analysis techniques can be split into two categories: qualitative and quantitative approaches. Qualitative methods try to find the causal dependencies between a hazard on system level and failures of individual components, while quantitative methods aim at providing estimations about probabilities, rates and severity of consequences. Many techniques are proposed for this purpose and are extensively described in (Ericson2005). These safety analyses are usually performed separately with independent tools. Consequently, they occur late in the design process when the design is already finalized and thus, miss the opportunity to influence design choices and decisions (Sharvia and Papadopoulos2010).

The purpose of our work is to provide a methodology to integrate safety analysis early in the design stage, when the first design models are available. The proposed methodology is based on pertinent semi-formal models built using SysML. The end goal of this work is to automate parts of the safety analysis process and, consequently, both reduce the time and cost and improve the quality of the system safety studies. The methodology allows system engineers to perform early validation of system safety requirements in the design process. In the scope of this paper, the preliminary work of identifying relevant information from design models and then using it to perform safety analysis is presented.

Dubois (Dubois2008) proposed to directly include safety requirements in the design process with SysML. To respect safety standards, the triplet requirement models, solution models and validation and verification (V&V) models are isolated. For this purpose, a SysML profile respecting safety standards called RPM (Requirement Profile for MeMVaTEX) was developed. The requirement stereotype of SysML is replaced by the MeMVaTEX requirement, by adding various properties such as "*verifiable*", "*verification type*", "*derived from*", "*satisfied by*", "*refined by*", "*traced to*", etc. In this work, traceability is assured between requirement models, between requirement and solution models, and between requirement and V&V models by using these properties. However, only the integration of safety requirements is considered in this work but safety analysis techniques (from which safety requirements are derived) are performed separately.

Another attempt more complete is proposed by P. David et al. (David2009, Cressent et al.2010, David et al.2010) work on the generation of an FMEA report from system functional behaviors written in SysML models, and on the construction of dysfunctional models by using the AltaRica language in order to compute reliability indicators. In their methodology called MéDISIS, they start with the automatic computation of a preliminary FMEA. The structural diagrams, namely Block Definition Diagram (BDD) and Internal Block Diagram (IBD), and the behavioral diagrams such as Sequence Diagram (SD) and Activity Diagram (AD) are analyzed in detail to give an exhaustive list of failure modes for each component and each function, with their possible causes and effects. Then the final FMEA report is created with help from experts in the safety domain. To facilitate a deductive and iterative method like MéDISIS, a database of dysfunctional behaviors is kept updated in order to rapidly identify failure modes in different analysis phases. The next step of their work is the mapping between SysML models and AltaRica data flow language, so that existing tools to quantify reliability indicators such as the global failure rate, the mean time to failure, etc. can be used directly on the failure modes identified in the previous step.

The work of David and his team is currently one of the most advanced research works about the integration of SysML and safety analyses.

3 Safety analysis integration in an MBSE approach with SysML

System engineering approach aims at realizing a system that satisfies customer needs. It focuses on defining customer needs and required functionality and then proceeds with design synthesis and system validation (INCOSE). To support systems engineering approach a tool must be able to model system requirements, behavior and structure and ensure consistency between these different views. SysML can represent the different aspects of systems (Friedenthal et al.2009):

- Requirements and their relationships to other requirements and to other modeling elements like components, test cases etc.
- Function-based, message-based (scenarios) and state-based behavior.
- Structure by modeling composition, and interconnection and interactions between components.
- Constraints on the physical and performance properties.

It also supports allocations between these different aspects, enhancing consistency and coherence between element models and making change impact evaluation easier.

The rich modeling capabilities of SysML made it a good candidate to support MBSE approach. This OMG standard is being widely used in both industrial and academic projects (a few examples can be found in (Wölkl and Shea2009, Cressent et al.2011, Piques and Adrianarison2012) because it provides a consistent, well-defined, and well-understood language to communicate the requirements and corresponding designs among engineers. The system model performed with SysML contains relevant information to support safety engineers in performing safety analyses from the early design phases.

Usually a design process begins with requirement definition and analysis. In this phase, the already known safety requirements are captured in the SysML model. In the second phase, system functions are identified from functional requirements and one or more functional architectures are defined and compared. Once a list of functions is available, functional hazard assessment can be performed in order to identify failure modes of each function and then the effects of each failure. Functions are thus classified according to their criticality and safety requirements are derived in order to eliminate risks or bring them to an acceptable level. These requirements specify allowable failure rates such as failures resulting in catastrophic effects are unlikely to occur. The requirements model is then updated and the whole process iterates until a satisfactory functional model is established. Then components are allocated to functions to define the physical structure of the system. These components shall satisfy the safety requirements derived from the functional hazard analysis. Component based safety analysis techniques, like Fault Tree Analysis, can then be applied based on the system architecture performed in SysML. Fault propagation cans then be deduced and allowed failure probabilities are distributed on different components in order to satisfy quantita-

tive safety requirements. The requirements are accordingly updated with new safety requirements and new induced functions may be added. The whole process shall be iterated again to assess system safety with the new changes and evaluate their impact on both performance and behavior of the system. The whole process can be summarized in Fig. 1.

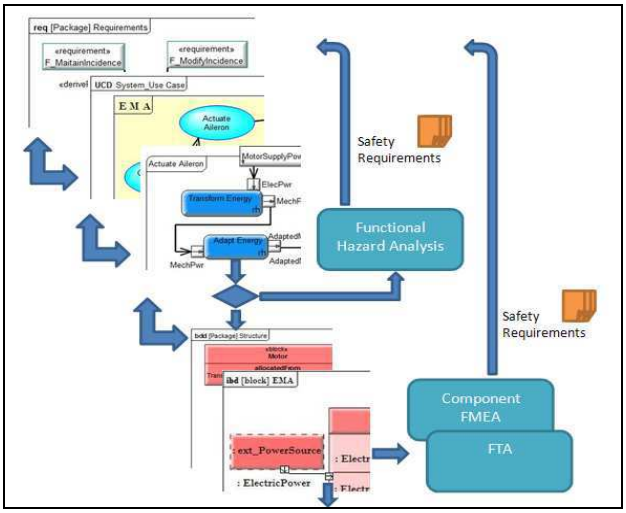

Fig. 1 Integration of safety analysis techniques in a SysML based MBSE Process

4 A case study

In this section, it will be shown how SysML model can be used for safety analysis in order to improve consistency and take safety aspects in consideration from the early design stages. The case study addressed in our paper is the wheel brake system of a fictitious aircraft described in the ARP 4761 standard – Appendix L (SAE-ARP 4761-1996).

First, requirements are captured within SysML. Then, functions are derived from functional requirements and captured within the SysML model. Main functions are then decomposed in sub-functions. An extract of the brake down of the aircraft functions is given in Fig. 2. At this early stage, safety analysis can already begin with analyzing functions. SysML functions model gives a list of functions that is helpful for safety engineers. In our example, an aircraft Functional Hazard Analysis (FHA) is performed to identify safety critical functions. The “Decelerate Aircraft on Ground” is identified as being safety critical since its failure could lead to catastrophic effects like the aircraft leaving the runway or crashing the build-

ings or equipment on the airport (SAE-ARP 4761-1996). “Decelerate Aircraft on Ground” function is broken down into sub-functions and is achieved by a number of aircraft sub-systems. Among these subsystems, the wheel brake system, which is the subject of our study, is the most influencing in decelerating the aircraft.

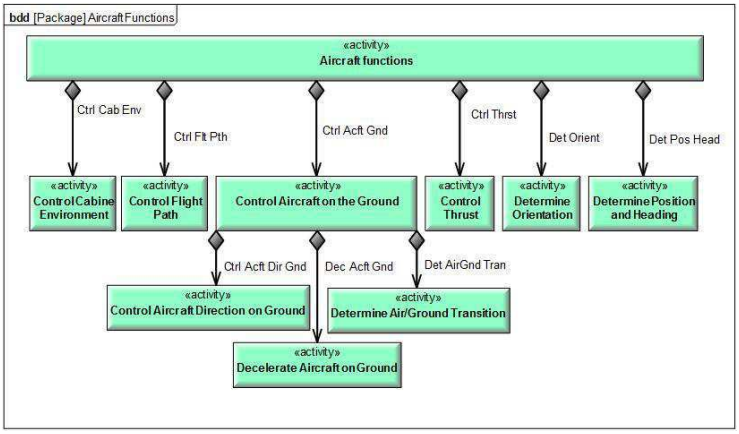

Fig. 2 Extract of aircraft level functions brake down

Safety requirements are derived to bring the effects of identified failure modes to acceptable levels. These requirements shall be satisfied by the physical system being developed. The choice of the system components and architecture is influenced by safety aspects resulting in less iteration and design changes.

The wheel brake systems shall satisfy the following requirement: “*The wheel-braking system shall be able to stop the aircraft safely in the landing phase, at high speeds and on different runway surfaces and climate conditions*”.

Thus, the architecture of the wheel brake system must be reliable and fault tolerant to minimize the risk of failure. Thus the wheel braking system is designed with redundant components: it is composed of two redundant hydraulic lines, a normal line that is first activated and an alternate one that is activated when the normal chain is inoperative. Each of the two systems has an independent power source. A supplementary power source, an accumulator, is added as an emergency power source (mandatory for the wheel-brake system in aircraft (Moir and Seabridge2001)). It provides the braking system with hydraulic power when all the other power sources are inoperative.

The different flow exchanges between components are given in Fig. 3 via a SysML Internal Block Diagram. For the sake of simplicity, the selection valve is not shown in this diagram. The selection valve is inserted across the two lines and checks the availability of power, i.e. hydraulic pressure above the threshold, on each of the two lines. The annunciating system feeds back the BSCU system with

the state of the hydraulic lines. The BSCU system itself feeds back the high level control unit with the state of the entire wheel brake system.

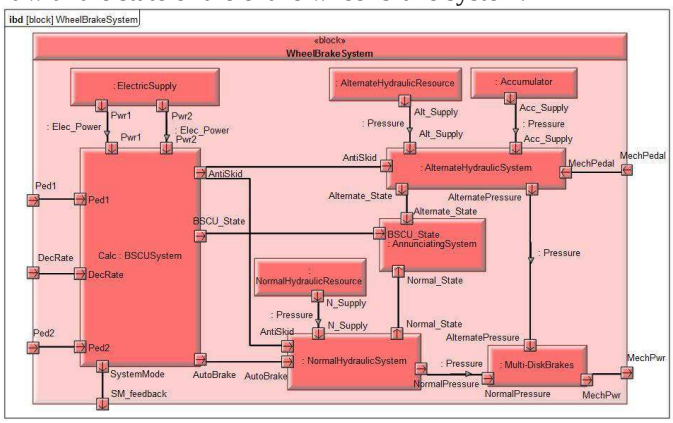

Fig. 3 Internal model of the wheel brake system.

Analyzing the interactions among system components, the failure propagation among components can be easily deduced and the Fault Tree built. The fault Tree detailing the “unannunciated loss of all wheel brakes” is given in Fig. 4.

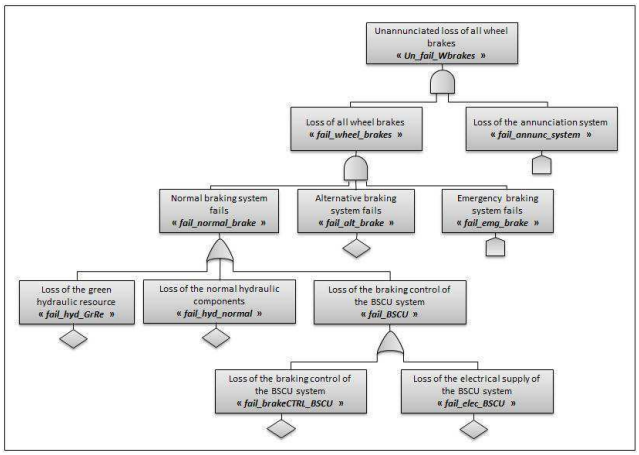

Fig. 4 Fault Tree for “unannunciated loss of all wheel brakes” failure.

Fault tree is used to analyze fault propagation through components. It can also be used for a quantitative analysis by allocating probabilities to different events.

5 Conclusion

This work is a contribution to the integration of safety analysis within SysML based MBSE approach. It was shown how SysML models can help in performing safety analysis by providing the information needed in a structured way. A case study was presented to illustrate the proposed approach.

In future works, the extension of SysML to support automatic generation of safety analysis datasheets will be considered. Automatic generation helps enhancing coherence and reduces gaps in the design process consequently reducing design errors as well as time and cost.

References

MIL-STD-1629A (1980). Procedure for performing a failure mode, effects and criticality analysis.

MIL-STD-882D (2000). Standard practice for system safety.

Cressent, R., David, P., Idasiak, V., and Kratz, F. (2010). Increasing reliability of embedded systems in a SysML centered MBSE process: Application to LEA project. In Workshop on Model Based Engineering for Embedded Systems Design, number 1. M-BED 2010.

Cressent, R., Idasiak, V., and Kratz, F. (2011). Prise en compte des analyses de la sûreté de fonctionnement dans l'ingénierie de système dirigée par les modèles SysML. Génie Logiciel, pages 33–39.

David, P. (2009). Contribution à l'analyse de sûreté de fonctionnement des systèmes complexes en phase de conception : application à l'évaluation des missions d'un réseau de capteurs de présence humaine. PhD thesis, Université d'Orléans.

David, P., Idasiak, V., and Kratz, F. (2010). Reliability study of complex physical systems using SysML. Reliability Engineering and System Safety, 95(4):431 – 450.

Dubois, H. (2008). Gestion des exigences de sûreté de fonctionnement dans une approche IDM. In Journées Neptune N°5, Paris, France.

Ericson, C. A. (2005). Hazard Analysis Techniques for System Safety. John Wiley & sons.

Friedenthal, S., Moore, A., and Steiner, R. (2009). A practical Guide to SysML, The Systems Modeling Langage. Morgan Kaufmann Publishers.

Moir, I. and Seabridge, A. (2001). Aircraft Systems, Mechanical Electrical and Avionics Subsystems Integration. Professionnal Engineering Publishing, second edition.

Perrow, C. (1981). Normal accident at Three Mile Island. Society, 18(5):17–26.

Piques, J.-D. and Adrianarison, E. (2012). SysML for embedded automotive systems: lessons learned. In Embedded real time Software and Systems ERTS, Toulouse, France.

SAE-ARP 4761-1996 Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment. ARP-4761.

Sharvia, S. and Papadopoulos, Y. (2010). Integrating compositional safety analysis and formal verification. In Petratos, P. and Sarrafzadeh, M., editors, Strategic Advantage of Computing Information Systems in Enterprise Management, pages 181–201.

Wölkl, S. and Shea, K. (2009). A computational product model for conceptual design using SysML. In Proceedings of the ASME 2009 International Design Engineering Technical Conferences & Computers and Information in Engineering Conference.